



Building *Governance* *Foundations* for Technology Startups in the GCC

A contextualised framework for founders, accelerators, and institutional stakeholders operating within the United Arab Emirates and the Kingdom of Saudi Arabia

\$35B

PROJECTED AI ECONOMIC
CONTRIBUTION TO GCC NON-OIL GDP

5600+

NEW TECH FIRMS REGISTERED IN
THE UAE

73%

GCC ORGANISATIONS THAT HAVE
PILOTED GEN AI APPLICATIONS

Why Governance Is No Longer *Optional* for GCC Startups

The Gulf Cooperation Council has undergone a structural transformation in its technology ecosystem. What was once a permissive, high-growth environment where regulatory compliance was secondary to speed-to-market has become one of the most rapidly institutionalising innovation landscapes in the world.

The UAE registered more than 5,600 new technology firms in a single quarter in 2024. Saudi Arabia attracted \$359 million in startup funding in the first three months of 2023 alone, representing the largest share of capital deployed across the MENA region. Yet a [McKinsey study](#) of 140 GCC C-suite leaders found that while 73% of organisations had piloted generative AI applications, only 11% had realised measurable value, with governance and data management cited as the principal impediments to value extraction.

This gap between deployment ambition and realised value is not primarily a technology problem. It is a governance problem. Startups that secure institutional capital, enter regulated markets, seek government partnerships, or aspire to cross-border scale increasingly require governance frameworks that match the sophistication of the ecosystems they operate within. This document provides the architecture for building precisely that.

The frameworks presented here are designed for practical application, not theoretical compliance. They are calibrated to the distinct institutional realities of the UAE and the Kingdom of Saudi Arabia, account for the free zone versus mainland jurisdictional duality, and are informed by the most recent legislative developments including the [UAE Cabinet's April 2025 AI governance legislation](#), the [UAE Securities and Commodities Authority's Chairman's Board Resolution No. 24 of 2025](#), and the full implementation of [Saudi Arabia's Personal Data Protection Law](#).

CRITICAL NOTE ON FREE ZONE GOVERNANCE

Technology startups incorporating in DIFC, ADGM, or Saudi Special Economic Zones should not treat the lighter-touch regulatory environment of these zones as grounds for governance minimalism. Institutional investors, government procurement officers, and corporate partnership counterparties will assess governance quality against the highest applicable standard, regardless of the formal jurisdiction of incorporation. Governance credibility is a function of practice, not solely of legal domicile.

The Regulatory Terrain: *UAE and KSA*

Any governance framework applied in the GCC must be grounded in an understanding of the distinct regulatory environments of the two dominant innovation markets. The UAE and KSA share a commitment to economic diversification and technology leadership, but their legal architectures, enforcement philosophies, and governance expectations differ in material ways.



United Arab Emirates

Jurisdictional Multiplicity

46 free zones operating under dedicated regulators, including DIFC and ADGM, each with distinct governance standards. Onshore companies are subject to federal law plus emirate-specific regulation, creating layered compliance obligations.

AI Governance Leadership

First nation globally to appoint a Minister of State for Artificial Intelligence (2017). National AI Strategy 2031, a 12-principle AI Charter (June 2024), and the establishment of Abu Dhabi's AI and Advanced Technology Council under Law No. 3 of 2024 set a comprehensive institutional architecture.

Corporate Governance Reform

SCA Resolution No. 24 of 2025 permits the combination of Chairman and CEO roles under strict conditions, signalling maturation of governance flexibility for high-growth companies, provided independent oversight structures are in place.

Data and Privacy

Federal Personal Data Protection Law applies across the onshore jurisdiction. DIFC and ADGM maintain their own data protection regimes aligned with international standards. Mandatory beneficial ownership registration under Cabinet Resolution No. 58 of 2020.

Corporate Tax Implications

Introduction of corporate tax with a 9% standard rate has elevated financial governance requirements. Entities with revenue at or above AED 50,000,000 must produce audited financial statements for tax compliance purposes.



Kingdom of Saudi Arabia

Vision 2030 Institutional Alignment

Corporate governance for technology startups in KSA is evaluated against Vision 2030 objectives. Government, sovereign wealth entities, and major institutional investors apply a strategic lens to governance assessments that extends well beyond formal compliance.

AI and Data Authority Architecture

SDAIA (Saudi Data and AI Authority) governs both data protection and AI adoption policy. The Personal Data Protection Law is now in full force, with detailed requirements for data localisation, consent management, and cross-border transfer. SDAIA's Generative AI Guidelines for both government and private sector entities apply.

Shariah Compliance Considerations

Shariah principles materially influence governance standards. Ethical frameworks governing financial instruments, contractual structures, and board-level conduct have direct operational relevance. Technology companies in financial services, healthcare, and consumer sectors must establish documented Shariah compliance procedures.

Saudisation and Workforce Governance

Nitaqat (workforce nationalisation) requirements are among the most structurally significant compliance obligations. Technology startups must develop progressive Saudisation roadmaps from the earliest stages of hiring. Non-compliance carries licence consequences.

Capital Market Authority Standards

Listed and pre-IPO entities must comply with CMA Corporate Governance Regulations, which establish detailed requirements for board composition, audit committee structure, the nomination and remuneration committee, and disclosure obligations on a comply-or-explain basis.

The Five Pillars of *Startup Governance* in the GCC

The governance architecture proposed here is structured around five interlocking pillars. Each pillar represents a domain of institutional integrity that technology startups must build progressively as they scale. No single pillar functions in isolation; the strength of the overall framework depends upon the coherence of all five working in concert.

PILLAR ONE

I

Board Architecture and Leadership Accountability

The composition, authority, and accountability mechanisms of the board of directors constitute the structural foundation of corporate governance. In the GCC context, this includes navigating the founder-control versus investor-protection tension, establishing meaningful independent oversight, and ensuring board competencies reflect the specific regulatory and cultural environment of UAE and KSA operations.

PILLAR TWO

II

Financial Integrity and Disclosure Standards

Financial governance encompasses the internal control environment, audit function independence, reporting quality, and transparency to investors and regulators. The introduction of UAE corporate tax, the full implementation of KSA's PDPL, and the regulatory expansion of beneficial ownership requirements have made financial governance a front-line compliance obligation, not merely a best-practice aspiration.

PILLAR THREE

III

Data Governance and Technology Risk

For technology companies, data governance is simultaneously a regulatory obligation, a competitive asset, and a source of existential risk. The UAE and KSA operate distinct but converging data protection regimes. AI-native startups must additionally contend with the emerging AI governance obligations now codified in both jurisdictions. This pillar encompasses data classification, privacy-by-design, algorithmic accountability, and cybersecurity risk management aligned with UAE NCSC standards.

PILLAR FOUR

IV

Stakeholder & Regulatory Relationship Management

In the GCC, the relationship between technology startups and government entities is categorically different from Western markets. Government bodies are simultaneously regulators, customers, investors, and strategic partners. Governance frameworks must include structured protocols for regulatory engagement, a policy monitoring function, and clear ownership of government relations at the executive level, with board visibility into regulatory risk.

PILLAR FIVE

V

ESG Integration and Social Licence

Environmental, Social, and Governance considerations are no longer peripheral to startup governance in the Gulf. Sovereign wealth fund investment criteria, Vision 2030's social transformation objectives, and the growing mandates of institutional co-investors require that technology startups articulate, measure, and report against ESG metrics from the growth stage onwards. This includes workforce nationalisation progress, carbon accountability, and ethical technology deployment policies.

CROSS-CUTTING

+

Cultural and Institutional Intelligence

Transcending all five pillars is the requirement for deep cultural and institutional intelligence. GCC governance does not operate as a Western regulatory framework transposed onto an Arab business environment. The institutional architecture is distinctive, the relationship between commercial entities and the state is substantively different, and the expectations of trust, discretion, and personal accountability held by senior government and institutional counterparties must be embedded into governance practice from first principles.

The *Governance Operating System* (GOS™)

A Three-Layer Model for Institutional Readiness in GCC Technology Startups

Governance in technology startups is often approached as a collection of structures, policies, and compliance obligations. This approach is incomplete.

In practice, governance functions as an operating system. It determines how decisions are made, how risk is managed, how information flows, and how the organisation responds under pressure.

The Governance Operating System (GOS) is a proprietary model that reframes governance not as a static framework, but as an integrated system composed of three interdependent layers. Institutional readiness is achieved not through the presence of individual components, but through the alignment of these layers in practice.

LAYER 1 • STRUCTURAL INTEGRITY

What exists

This layer represents the formal architecture of governance within the organisation.

It includes:

- Board composition and independence
- Legal and shareholder structures
- Financial reporting systems and audit mechanisms
- Data governance frameworks and policies
- ESG commitments and formal disclosures

Structural integrity answers a foundational question:

Does the organisation have the necessary governance components in place to operate credibly within its regulatory and investment environment?

At early stages, this layer is defined by completeness. At later stages, it is defined by robustness and alignment with institutional standards.

LAYER 2 • OPERATIONAL DISCIPLINE

How it functions

This layer reflects the extent to which governance structures are actively used, maintained, and embedded into day-to-day operations.

FRAMEWORK

It includes:

- Quality and consistency of board engagement
- Reliability and cadence of reporting
- Execution of risk management processes
- Enforcement of policies and internal controls
- Responsiveness to regulatory and operational events

Operational discipline answers a second question:

Are governance structures consistently applied in practice, or do they exist only in documentation?

This is the layer where most governance systems fail. Structures are often present, but inconsistently applied.

LAYER 3 • INSTITUTIONAL BEHAVIOUR

How it holds under pressure

This layer captures how governance manifests in moments of stress, ambiguity, and strategic decision-making.

It includes:

- Decision-making under uncertainty
- Escalation of risk and transparency to the board
- Alignment between leadership behaviour and stated governance principles
- Handling of regulatory scrutiny and stakeholder pressure
- Integrity of actions during periods of rapid growth or crisis

Institutional behaviour answers the most critical question:

Does the organisation behave in a way that reflects institutional-grade governance under conditions of stress, growth, or scrutiny?

This layer cannot be fabricated. It is observable over time.

Layer	Strong Signal	Weak Signal
Structural Integrity	Complete and stage-appropriate governance architecture	Missing or misaligned core structures
Operational Discipline	Consistent execution of governance processes	Irregular reporting and reactive management
Institutional Behaviour	Transparent, accountable decision-making under pressure	Governance breakdown during stress events

Governance by *Lifecycle Stage*

A governance framework is not a static document. It must evolve with the company, anticipating regulatory triggers, capital events, and market expansion decisions. The following lifecycle architecture maps governance obligations and best-practice interventions to the four principal stages of a technology startup's development in the GCC context.

STAGE I · PRE-SEED TO SEED

Governance Foundations: Structure Before Scale

The governance infrastructure established at incorporation shapes the company's trajectory for years. Founders frequently treat early legal and governance decisions as administrative burdens to be minimised; this is a strategic error that becomes progressively more expensive to correct. Critical early decisions include jurisdictional selection (onshore versus free zone in UAE; mainland versus SEZ in KSA), the shareholder agreement architecture, and the initial board formation. In the UAE, the corporate governance expectations of DIFC and ADGM are meaningfully higher than those of onshore free zones, and selecting these jurisdictions signals institutional intent to future investors. At this stage, the non-negotiable governance requirements are documented founder agreements with vesting schedules, a data protection policy consistent with the applicable jurisdiction's law, initial beneficial ownership registration where required, and at minimum one external board observer with relevant domain expertise.

Shareholder agreement

Founder vesting

Beneficial ownership registration

Initial data protection policy

Jurisdictional decision

STAGE II · SERIES A TO SERIES B

Formalisation: From Informal Practice to Documented Process

The transition from seed to institutional capital is the moment at which governance formality becomes non-negotiable. Series A and B investors, particularly those from sovereign wealth funds, family offices, or international institutional sources, will conduct governance due diligence as a material component of their investment assessment. In the GCC, this due diligence will specifically assess: the independence and composition of the board (including at minimum one truly independent director with no financial or personal relationships with the founding team); the quality and regularity of board minutes and resolutions; the robustness of the financial reporting cycle including alignment with IFRS standards; the structure and independence of any audit function; and the depth of the data governance and cybersecurity framework. The UAE's enhanced disclosure obligations introduced in 2024–2025 require companies to begin building the reporting infrastructure that regulators and investors will expect at later stages.

Independent director appointment

Board charter & Terms of Reference

Internal audit or external equivalent

IFRS-aligned financial reporting

Data protection officer

Investor relations protocol

STAGE III · SERIES C AND GROWTH

Institutional Alignment: Governance as Strategic Enabler

At the growth stage, governance moves from a compliance function to a strategic asset. Companies at this stage typically have government procurement relationships, are operating across multiple GCC markets, and are preparing for either strategic exit, strategic partnership with a sovereign entity, or capital market preparation. The governance priorities shift accordingly. Board composition should include directors with direct regulatory experience in the primary markets of operation. An audit committee with formal terms of reference and an independent chair becomes essential. Risk governance must expand to include a documented enterprise risk management framework. The most strategically important governance intervention at this stage in the GCC context is the formalisation of government relations governance: who owns the relationship with each regulatory authority, what is the protocol for regulatory engagement, and how does board oversight of regulatory risk function. This is particularly critical in KSA, where Vision 2030-aligned entities are subject to heightened scrutiny of governance quality as a condition for sustained government partnership.

Audit committee (Formal Charter)

Enterprise Risk Management Framework

Government Relations Governance Protocol

ESG Reporting Framework

Whistleblower policy

Anti-Bribery & Anti-Corruption Framework

Transfer pricing documentation (UAE CT)

STAGE IV · PRE-IPO AND EXIT

Capital Markets Readiness: Institutional-Grade Governance Architecture

Companies preparing for listing on DFM, ADX, Tadawul, or international exchanges from a GCC base must meet the highest standard of governance formalisation in the region. The CMA Corporate Governance Regulations in KSA and the SCA Governance Guide (as amended by Resolution No. 24 of 2025) in the UAE establish detailed requirements for listed companies. Pre-IPO governance preparation should begin at minimum 18 to 24 months before the anticipated listing date. Critical requirements include the formation of a formally constituted nomination and remuneration committee; a board diversity policy addressing gender and experience composition; a robust related-party transaction policy with board-level approval thresholds; a comprehensive investor relations function with documented disclosure policies; and a sustainability report aligned with internationally recognised ESG reporting standards. In KSA, the comply-or-explain principle that governs the CMA Corporate Governance Regulations means that substantive non-compliance must be disclosed and justified in the annual report, placing premium on proactive alignment rather than reactive explanation.

Nomination & Remuneration Committee

Board diversity policy

Related-Party Transaction Controls

Sustainability Report (ESG)

Investor relations

Board effectiveness evaluation

Director liability insurance

AI Governance: *The Critical Frontier*

Technology startups operating in the GCC whose products incorporate artificial intelligence face a governance obligation that extends well beyond the general corporate framework. The AI governance landscape in both UAE and KSA is moving from strategic guidelines to enforceable obligations with material speed, and companies that treat AI governance as a future concern are already behind.

REGULATORY TRAJECTORY

The UAE Cabinet's decision in April 2025 to establish a comprehensive AI-linked legislative framework represents the most significant regulatory development for GCC technology companies since the introduction of corporate tax. While none of the GCC states has yet enacted an omnibus AI statute comparable to the EU AI Act, the regulatory direction is unambiguous. Startups that build AI governance infrastructure now will face structurally lower transition costs when binding legislation materializes.

Required Elements of an AI Governance Framework

01 **AI Ethics Policy and Accountability Structure**

A documented AI ethics policy aligned with the UAE AI Charter's 12 principles, including algorithmic bias mitigation, human oversight mechanisms, and clear accountability ownership at the executive level. In KSA, alignment with SDAIA's Generative AI Guidelines for the private sector is the applicable reference standard.

02 **Model Risk Management**

Technology startups deploying AI models in regulated sectors (fintech, healthtech, regtech, insuretech) must implement a model risk management framework that documents model development, validation, deployment, and retirement processes. Qatar's Artificial Intelligence Guidelines, the only legally binding AI governance instrument in the GCC currently require financial sector entities to maintain precisely this infrastructure, and its requirements represent a forward-looking standard for the broader region.

03 **Data Governance for AI Training and Inference**

The intersection of AI deployment and data protection law is the most legally complex governance domain for GCC technology companies. AI models trained on personal data are subject to both UAE and KSA personal data protection law requirements around lawful basis, data minimisation, purpose limitation, and cross-border transfer restrictions. Data governance for AI must address the provenance, classification, and retention policies for training data as a distinct governance function from general data management.

04 **Algorithmic Accountability and Transparency**

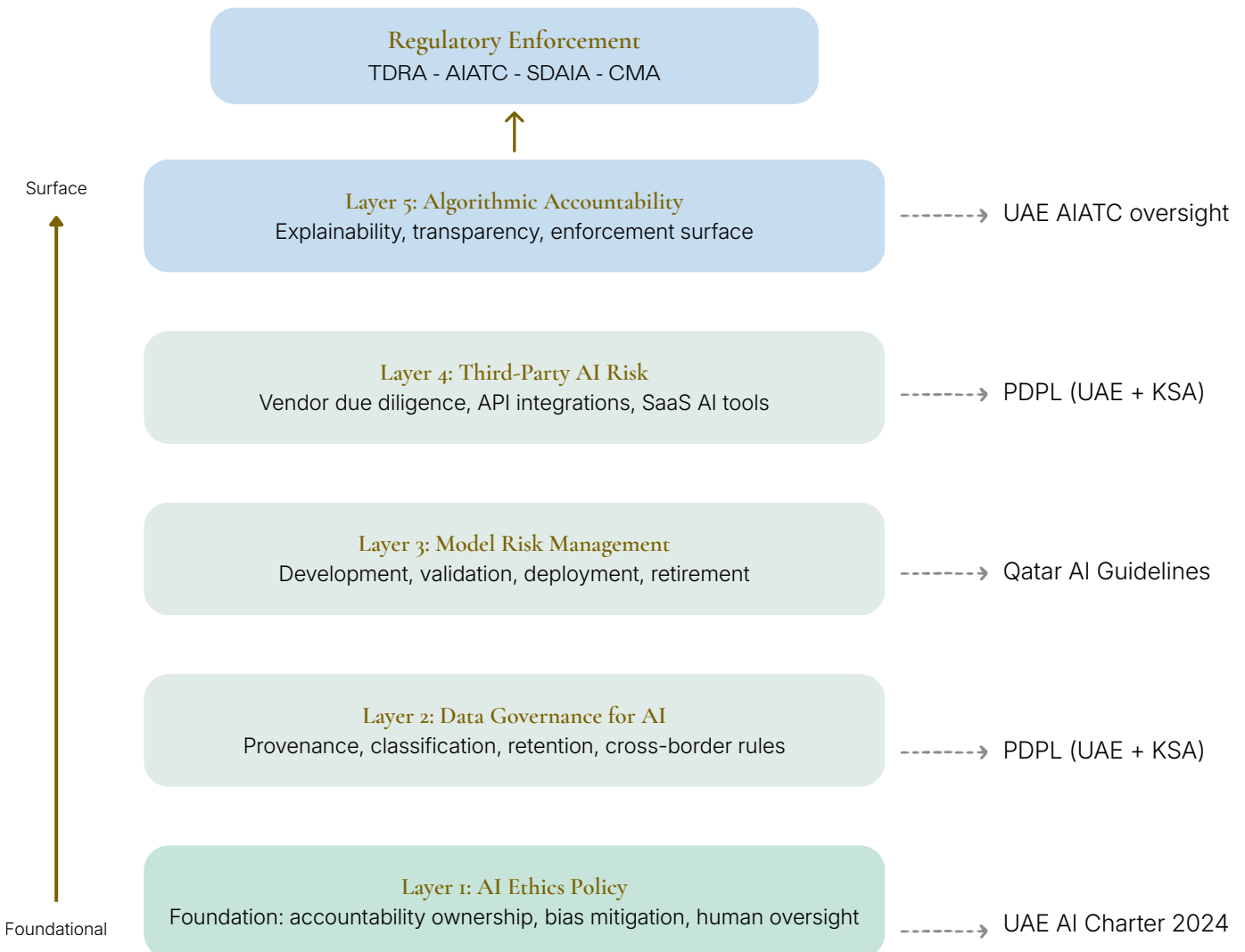
Companies deploying AI systems that make or materially influence decisions affecting individuals in credit, insurance, employment, healthcare, or government services must establish explainability protocols. The UAE's International Stance on Artificial Intelligence Policy and the Abu Dhabi AIATC's oversight remit both indicate that transparency and human oversight are enforcement priorities, not aspirational principles.

05 Third-Party AI Risk Management

The governance obligation does not stop at a company's own AI systems. Technology startups that integrate third-party AI APIs, foundation models, or AI-powered SaaS tools into their products carry a governance responsibility for the downstream risks those integrations introduce. Vendor due diligence for AI tools should include an assessment of the vendor's own governance standards, data handling practices, and alignment with applicable GCC regulatory requirements.

HIGH-RISK SECTOR ALERT

AI-powered startups operating in financial services, healthcare, education, or government technology in the UAE or KSA should anticipate sector-specific AI governance requirements being published by the respective sectoral regulator, i.e., CBUAE, MOH, MOHE, or MISA, within the near-term regulatory horizon. Companies in these sectors should not wait for those instruments to be published before building governance infrastructure consistent with the direction of travel.



The Governance *Accountability Matrix*

Effective governance requires clarity about who is responsible for what, and at what level of the organisation. The following matrix establishes the accountability architecture for the five core governance pillars across three organisational levels: **Board, Executive Leadership, and Operational Function**.

Domain	Board Accountability	Executive Ownership
<p>Board Architecture</p> <p>Board self-governance, director appointment, independence assessment, performance evaluation</p>	<p>Full board responsibility. Governance committee recommended at Series B+. Chair leads annual board effectiveness evaluation.</p>	<p>CEO provides board with strategic context and operational updates. Company Secretary manages board administration and compliance calendar.</p>
<p>Financial Integrity</p> <p>Audit oversight, financial reporting quality, internal controls, tax compliance</p>	<p>Audit committee (or full board at early stage) reviews and approves financial statements. Approves appointment and remuneration of external auditors.</p>	<p>CFO owns financial reporting and internal control environment. Head of Finance manages day-to-day compliance with tax, audit, and regulatory reporting obligations.</p>
<p>Data and Technology Risk</p> <p>Cyber risk oversight, data governance policy, AI ethics oversight</p>	<p>Board (or risk committee) receives quarterly cybersecurity risk update. Approves data governance policy and AI ethics policy at Group level.</p>	<p>CTO or CISO owns technical security controls. DPO (where appointed) owns data protection compliance. AI Ethics Lead owns algorithmic accountability programme.</p>
<p>Regulatory Relations</p> <p>Regulatory risk oversight, licence compliance, policy engagement strategy</p>	<p>Board is notified of all material regulatory interactions and receives regulatory risk update at minimum semi-annually. Board approves engagement with regulators on matters of significant policy consequence.</p>	<p>CEO or designated Government Relations Director owns primary regulatory relationships. Legal Counsel manages licence compliance and submission calendars.</p>
<p>ESG and Social Licence</p> <p>ESG strategy and target approval, workforce nationalisation oversight, sustainability reporting</p>	<p>Board approves ESG policy and targets. Receives annual ESG performance report. Oversight of workforce nationalisation progress (Emiratization/Saudisation) given regulatory consequence.</p>	<p>Chief People Officer owns Nitaqat/Emiratization programmes and reports progress quarterly. Sustainability lead (where appointed) owns ESG data collection and reporting cycle.</p>

Governance *Escalations and Reporting* Logic

Effective governance requires not only clarity of roles, but clarity of escalation and reporting pathways. The allocation of responsibility across board, executive, and operational levels must be supported by structured mechanisms that determine when issues are escalated and how they are addressed.

Operational issues should be managed at the executive level where they fall within defined risk tolerances and established policy frameworks. Routine compliance matters, financial reporting processes, and standard regulatory interactions should remain within management ownership, with periodic reporting to the board.

Matters that involve material financial exposure, regulatory risk, reputational impact, or deviation from approved strategy must be escalated to the board. This includes significant cybersecurity incidents, data breaches, regulatory investigations, and material changes in financial performance.

The board should receive structured reporting on a defined cadence. Financial performance should be reviewed quarterly at minimum. Regulatory and compliance updates should be provided semi-annually or more frequently where exposure is high. Cybersecurity and technology risk should be reported at least quarterly, particularly for AI-enabled or data-intensive businesses.

Escalation should not be reactive. Governance systems must be designed to identify emerging risks early and ensure that the board has sufficient visibility to exercise oversight before issues become operational crises.

Escalation Threshold Framework

Organisations should define clear thresholds that determine when an issue remains at management level and when it must be escalated to the board. The absence of defined thresholds is one of the most common causes of delayed escalation and governance failure.

A simple escalation framework can be structured across **four dimensions**:

- **Financial Impact:** Any issue with actual or potential financial exposure above a defined threshold, for example 5 to 10 percent of monthly revenue, should be escalated.
- **Regulatory Exposure:** Any interaction involving a regulator beyond routine filings, including inquiries, notices, or investigations, should be escalated.
- **Reputational Risk:** Issues that could materially affect brand perception, customer trust, or government relationships should be escalated regardless of financial impact.
- **Operational Disruption:** Incidents that affect core product functionality, data integrity, or service continuity should be escalated if resolution exceeds predefined timelines.

Thresholds should be documented, reviewed annually, and aligned with company stage and sector.

Governance Escalation Matrix

Scenario	Management Action	Board Involvement
Minor compliance deviation	Corrective action internally	Included in periodic reporting
Financial variance within tolerance	Managed by CFO and leadership	Reviewed in quarterly board meeting
Regulatory inquiry or notice	Immediate legal review and response	Board notified within 48 hours
Data breach or cybersecurity incident	Activate incident response plan	Emergency board briefing required
Strategic deviation or major risk event	Executive decision with documentation	Board approval or guidance required

Governance Checklist: Key Questions

Founders should periodically assess whether escalation and reporting systems are functioning effectively. Key questions include:

1. Are escalation thresholds clearly defined and understood across the leadership team
2. Does the board receive consistent and structured reporting
3. Are risks identified early, or only after escalation becomes unavoidable
4. Is there clear ownership of regulatory and compliance responsibilities
5. Do board discussions reflect real oversight or only formal updates

If these questions cannot be answered confidently, governance structures are likely insufficient for the company's current stage.

Governance Maturity *Assessment Indicators*

Governance maturity cannot be assessed solely by the existence of formal structures. It is reflected in the consistency, quality, and credibility of governance practices over time. At early stages, maturity is indicated by clarity of ownership, alignment between founders, and the presence of basic legal and data governance frameworks. At growth stages, maturity is reflected in the quality of board engagement, the reliability of financial reporting, and the depth of risk management processes.

For institutional stakeholders, key indicators of governance maturity include the independence and effectiveness of the board, the transparency of decision-making processes, and the organisation's ability to respond to regulatory and operational challenges with discipline.

Observable signals of strong governance include consistent and well-documented board deliberation, proactive regulatory engagement, and alignment between stated policies and actual operational behaviour. Conversely, governance gaps are often visible in reactive decision-making, inconsistent reporting, and the absence of clear accountability structures.

Governance maturity is not binary. It is progressive, and instead, it must be evaluated in the context of organisational stage, sector, and regulatory exposure.

What to Look For at Each Stage:

Early-Stage Foundations

- Clear ownership across founders and leadership
- Documented agreements and decision-making rights
- Basic data protection and compliance structures

At this stage, maturity is defined by clarity and alignment, not complexity.

Growth-Stage Structures

- Active and independent board engagement
- Reliable and timely financial reporting
- Defined risk management processes

Here, maturity is visible in consistency and discipline.

Scale-Stage Credibility

- Independent and effective board oversight
- Transparent decision-making processes
- Strong regulatory and stakeholder relationships

At this stage, maturity is reflected in external trust and institutional confidence.

Common *Governance Failures* in GCC Startups and How to Avoid Them

The following observations are drawn from the patterns of governance failure most commonly encountered in the GCC startup ecosystem. Each represents a structural or behavioural failure mode with material consequences for company resilience, investor confidence, and regulatory standing.

Treating Governance as a Fundraising Event

The most pervasive governance failure in the GCC startup ecosystem is the practice of installing governance infrastructure only when a fundraising round or due diligence process requires it. This approach produces governance artefacts such as board minutes, shareholder agreements, data protection policies, that are superficially compliant but operationally inert. Regulators, institutional investors, and sophisticated counterparties have developed significant capability to distinguish between governance that is practised and governance that is performed. The operational culture of a company, the evidence of genuine board deliberation in meeting minutes, the quality and consistency of financial reporting, and the behaviour of management under pressure are all observable indicators of governance quality that cannot be fabricated retrospectively.

THE GOVERNANCE-AS-A-CULTURE PRINCIPLE

Governance is not a set of documents. It is the aggregate of the decisions made, the processes followed, and the behaviours exhibited over time. A board charter filed with a regulatory authority but never operationalised is worse than no board charter: it demonstrates the intention to mislead. Build governance practices before building governance documentation, and the documentation will reflect institutional reality rather than institutional aspiration.

Under-Investing in Independent Oversight

Founders operating in the GCC frequently underestimate the strategic value of genuinely independent board directors, as opposed to investor-nominated directors who, regardless of their legal independence classification, represent a specific capital interest rather than the company's broader institutional health. An independent director with deep knowledge of the UAE or KSA regulatory environment, established relationships with relevant government authorities, and professional obligations of impartiality provides a governance resource that cannot be replicated by legal counsel, advisors, or investor representatives. The cost of this oversight is substantially lower than the cost of the regulatory, reputational, or investor relationship failures it prevents.

Neglecting the Cultural Dimension of Board Conduct

Corporate governance frameworks developed in the United States or the United Kingdom do not translate unmodified into the GCC context. Board conduct, decision-making processes, the management of disagreement, the relationship between board members and executive management, and the role of personal relationships and trust in institutional decision-making all operate according to distinct cultural norms in the Gulf. A board that operates as though it is convened in a Western institutional context, with adversarial challenge, public disagreement, and formal majority voting as primary tools of oversight, will be less effective in the GCC environment than one that understands how to exercise rigorous oversight within the relational and cultural frameworks that govern professional conduct in the region.

Inadequate Workforce Localisation Governance

The Nitaqat system in Saudi Arabia and Emiratisation requirements in the UAE represent among the most operationally consequential regulatory obligations for technology startups. Both regimes carry licence and commercial consequences for non-compliance, and both are subject to regular tightening of requirements. Technology companies frequently underestimate the structural challenge of meeting localisation targets in technical roles where the local talent pool is deepening but not yet at scale. Governance of these programmes must include a dedicated ownership structure within the People function, regular board-level reporting on progress, and a long-term talent development strategy and not merely a hiring metric.

Failure to Anticipate Cross-Jurisdictional Governance Complexity

Many GCC technology startups incorporate in both UAE and KSA, operate across multiple free zones, and maintain international entity structures for holding, IP, or capital purposes. The governance complexity of multi-jurisdictional structures is routinely underestimated. The interaction between UAE federal law, emirate-specific regulation, DIFC or ADGM frameworks, KSA Companies Law, and the requirements of international investor jurisdictions creates a compliance matrix that requires professional governance counsel and not merely administrative management. The transfer pricing documentation requirements introduced under the UAE corporate tax regime are a single but significant example of a cross-jurisdictional governance obligation that has caught many startups without adequate preparation.

Governance as a Fundraising Event	Regulatory	<div style="width: 60%;"><div style="background-color: red; height: 10px;"></div></div>	Investor	<div style="width: 85%;"><div style="background-color: blue; height: 10px;"></div></div>	Operational	<div style="width: 65%;"><div style="background-color: gray; height: 10px;"></div></div>	Critical
Under-investing in independent oversight	Regulatory	<div style="width: 70%;"><div style="background-color: red; height: 10px;"></div></div>	Investor	<div style="width: 80%;"><div style="background-color: blue; height: 10px;"></div></div>	Operational	<div style="width: 30%;"><div style="background-color: gray; height: 10px;"></div></div>	Critical
Neglecting cultural board conduct	Regulatory	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>	Investor	<div style="width: 60%;"><div style="background-color: blue; height: 10px;"></div></div>	Operational	<div style="width: 80%;"><div style="background-color: gray; height: 10px;"></div></div>	Elevated
Inadequate workforce localisation governance	Regulatory	<div style="width: 95%;"><div style="background-color: red; height: 10px;"></div></div>	Investor	<div style="width: 60%;"><div style="background-color: blue; height: 10px;"></div></div>	Operational	<div style="width: 65%;"><div style="background-color: gray; height: 10px;"></div></div>	Critical
Cross-jurisdictional complexity underestimated	Regulatory	<div style="width: 80%;"><div style="background-color: red; height: 10px;"></div></div>	Investor	<div style="width: 70%;"><div style="background-color: blue; height: 10px;"></div></div>	Operational	<div style="width: 80%;"><div style="background-color: gray; height: 10px;"></div></div>	Critical

Recommendations for *Accelerators* and *Government Bodies*

The quality of governance in GCC technology startups is not solely the responsibility of founders. Accelerators, innovation programmes, government entities, and institutional investors collectively shape the governance expectations and capabilities of the ecosystem. The following recommendations are addressed to these institutional actors.

01 **Embed Governance Curriculum into Accelerator Programmes**

Governance should be treated as a core competency in accelerator education, not a peripheral workshop. The most effective interventions combine conceptual instruction with direct access to governance practitioners such as former regulators, experienced independent directors, and senior legal advisors, who can provide contextually relevant guidance. The GCC Board Directors Institute and the DIFC-hosted governance resources represent accessible institutional anchors for this curriculum.

02 **Establish Governance Benchmarks as Investment Criteria**

Government-backed investment vehicles, including Mubadala Ventures, Saudi Venture Capital Company, and affiliated entities, are increasingly incorporating governance quality into their investment criteria. Formalising governance benchmarks as explicit due diligence requirements rather than implicit assessments, creates a market signal that incentivises governance investment across the ecosystem.

03 **Create Regulatory Sandbox Access Linked to Governance Standards**

The ADGM and DIFC regulatory sandbox programmes, and SAMA's fintech sandbox in KSA, could strengthen ecosystem-wide governance by linking sandbox access to demonstrated governance quality. Companies admitted to sandbox environments with robust governance frameworks are more likely to produce commercially viable, regulatorily coherent outputs that benefit the broader ecosystem.

04 **Develop a GCC-Specific Governance Standard for Technology Startups**

The GCC currently lacks a unified, publicly endorsed governance standard calibrated specifically for technology startups, analogous to the UK Corporate Governance Code but contextualised to the GCC regulatory environment, the role of government as commercial partner, and the cultural dimensions of institutional conduct in the Gulf. Development of such a standard, endorsed by the GCC Board Directors Institute, SDAIA, and the UAE's TDRA, would provide a credible, accessible reference point for founders, investors, and regulators alike.

05 **Invest in the Pipeline of Independent Directors with Technology and Regional Expertise**

One of the most material constraints on governance quality in the GCC startup ecosystem is the limited supply of independent directors who combine technology sector expertise with deep knowledge of the regional regulatory environment. Government and accelerator bodies should actively support director development programmes, board diversity initiatives, and professional development pathways that expand this talent pool.

Governance as a *Competitive Advantage*

The GCC technology ecosystem stands at an inflection point. The ambition is extraordinary: sovereign-scale capital deployment, national AI strategies with global reach, economic diversification targets that redefine what these economies produce and export. The governance infrastructure being built today will either support or constrain the realisation of that ambition.

Startups that treat governance as an institutional investment and not a compliance cost, will occupy a structurally advantaged position as the ecosystem matures. They will attract higher-quality institutional capital, navigate regulatory transitions with lower friction, sustain government partnerships with greater depth, and build organisations that are resilient to the specific failure modes that are endemic to high-growth environments operating under conditions of regulatory uncertainty.

The frameworks presented in this document are neither comprehensive nor static. They represent a coherent starting architecture, calibrated to the current regulatory and institutional environment of the UAE and KSA, and designed to evolve as that environment continues its rapid development. The most important governance decision any GCC technology founder can make is to begin building that architecture now; before the fundraising round that demands it, before the regulatory event that requires it, and before the commercial partnership that is conditional upon it.

Scope and Limitations

This framework is designed as a reference architecture for governance in technology startups operating within the UAE and the Kingdom of Saudi Arabia. It reflects the regulatory environment, institutional structures, and market dynamics as of Q2 2026.

The framework does not constitute legal, regulatory, or financial advice. Companies should seek qualified professional counsel when making jurisdictional, compliance, or structural decisions.

Regulatory frameworks in the GCC are evolving rapidly, particularly in areas related to artificial intelligence, data protection, and financial services. Organisations should continuously monitor regulatory developments and update governance practices accordingly.

The framework is not exhaustive. It is intended to provide a structured starting point that can be adapted based on sector-specific requirements, cross-border operations, and the strategic objectives of the organisation.

This framework is produced for distribution to founders, accelerators, and institutional stakeholders operating within the GCC technology ecosystem. It is intended as a reference architecture and does not constitute legal, regulatory, or financial advice. All regulatory references reflect the state of applicable law as of Q2 2026.

To work with us or know more, please reach out at: inadkarni@pearlinitiative.org